REMARKS

This Application has been carefully reviewed in light of the Official Action mailed February 1, 2001. In order to advance prosecution of this case, Applicant amends Claims 1, 3, 6, 9, 10, 11, 12, 13, and 15 and adds new Claims 25 and 26. Applicant respectfully submits that no new matter has been added. Applicant respectfully requests reconsideration and favorable action in this case.

Information Disclosure Statement

The Examiner has not considered non-patent documents in IDS paper No. 2, PTO-1449, pp. 2, 3 and 4-10 and requests that Applicant point out which particular documents should be considered by the Examiner for the claimed invention.

Applicant respectfully declines to point out which particular documents should be considered by the Examiner for the claimed invention, and respectfully submits that no provision of the Code of Federal Regulations or the Manual of Patent Examining Procedure (M.P.E.P.) suggests that the Examiner may require the Applicant to do so. In fact, the M.P.E.P. clearly states that the Examiner may not make such a requirement. Section 2004 of the M.P.E.P. informs applicants that they may "highlight" documents that "are known to be of the most significance," but this statement is merely "presented as [a] helpful suggestion[ ] for avoiding duty of disclosure problems," and "compliance with the [suggested] procedure[ ] may not be required." Accordingly, Applicant respectfully submits that the Examiner may not require the Applicant to identify particular references cited in the IDS.

Applicant respectfully submits that it would be improper to highlight any of the cited references. All documents in the IDS have been brought to Applicant's attention (i.e., are

known by Applicant) and are considered relevant enough to be included in the IDS. Nothing more is required of Applicant.

Section 102 Rejections

The Examiner rejects Claims 1-8 and 15 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,919,247 issued to Van Hoff, et al. ("*Van Hoff*"). Applicant respectfully traverses these rejections, as discussed more fully below, and respectfully requests reconsideration and favorable action with respect to these Claims.

Claim 1, as amended, recites automatically downloading from a remote site any update for the intrusion detection system, installing a downloaded update to generate a second version of the intrusion detection program and operating the second version of the intrusion detection program. *Van Hoff* does not teach distribution of an intrusion detection program and accordingly does not anticipate amended Claim 1. Thus, Claim 1 and its dependant Claims 2, 4, and 6-8 are patentable over the cited art.

Claim 3 has been amended to be in independent form. Claim 3 is patentable over the cited art because the art fails to teach aging the first version of the program as recited by Claim 3. *Van Hoff*, as relied upon by the Examiner, teaches a "minimal delay" before a client issues a further request for a channel. *Van Hoff*, Col. 10, ll. 24-32. This minimal delay is used to reduce the load on the server. *Id.* There is no teaching of aging a program, such that, for example, the program determines when it may be in need of updating. Therefore, Claim 3 is not anticipated by *Van Hoff*.

Claim 15 has been amended to be in independent form. *Van Hoff*, as relied upon by the Examiner, teaches that "a content provider can store a web-site . . . in a channel." In

contrast, there is no teaching in *Van Hoff* for automatically downloading an *update* for a program *from* a web site. These are fundamentally different concepts. Therefore, Claim 15 is not anticipated by *Van Hoff* and patentable over the cited art.

Section 103 Rejections

The Examiner rejects Claims 9, 10-14 and 16-24 under 35 U.S.C. § 103(a) as being unpatentable over *Van Hoff* and in view of "common wisdom practice in the art." Applicant respectfully traverses these rejections, as discussed more fully below, and respectfully requests reconsideration and favorable action with respect to these Claims.

Claim 9 has been amended to be in independent form. Applicant respectfully submits that nothing in the cited art suggests, as recited by Claim 9, restoring a first version of a program for operation at a network site when, after installation of a downloaded update, it is determined that the update is operating incorrectly. Applicant respectfully disputes Examiner's assertion that *Van Hoff* suggests such restoring. Instead, *Van Hoff*, as relied upon by the Examiner, merely teaches the use of a "holding space" to "store data received as part of update replies." *Van Hoff*, col. 9, ll. 11-12. The update reply commands are not immediately applied because "*modification of program code or data* may corrupt channel application 153 *if* that application is running at the time of the updates." *Van Hoff*, col. 9, lines 19-22 (emphasis added). "Instead the changes from holding space 156 are applied either when channel application 153 terminates, or when channel application 153 explicitly requests so, thus bringing the channel up to date." Col. 9, lines 23-25. Thus, *Van Hoff*'s teachings are limited to holding off an update until an application is ready. There is no teaching of

restoring a first version of a program, much less determining whether a second version is operating correctly. In addition, because the holding space of *Van Hoff* is for unapplied updates, there is no "means" for retrieving a previous version as asserted by the Examiner.

To the extent that the Examiner relies on "common wisdom practice" for elements of Claim 9 or for a suggestion to modify the cited art, Applicant respectfully traverses this assertion and requests that the Examiner cite a reference in support of the Examiner's position pursuant to M.P.E.P. § 2144.03.

Claim 10 has been amended to be in independent form. With respect to the patentability of Claim 10, there is no suggestion or motivation in the cited art to add "distributing the downloaded update to a disparate network site operating the first version." In contrast, in *Van Hoff*, a transmitter process calculates *client-specific* differences and a set of commands used to update the channel data. Col. 5, lines 22-29. Distributing the downloaded update to a disparate network site and without such client-specific calculation is not suggested by *Van Hoff*. Moreover, to the extent that the Examiner intends to take official notice that such an addition would be "apparent" and "common wisdom practice" for elements of Claim 10 or for a suggestion of the prior art, Applicant respectfully traverses this assertion and requests that the Examiner cite a reference in support of the Examiner's position pursuant to M.P.E.P. § 2144.03.

Claim 11 has been amended to be in independent form. Similar to Claim 1, Claim 11 recites restoring a first version of a program for operation at a network site when, after installation of a downloaded update, it is determined that the update is operating incorrectly. Similar to Claim 10, Claim

11 recites distributing the downloaded update to a disparate network site operating the first version. Therefore Claim 11 is patentable.

Claim 12 has been amended to be in independent form. The abstract of *Van Hoff*, relied upon by the Examiner, teaches against broadcasting distribution of software. The abstract teaches that "the client initiates each update request without requiring any special broadcast networking infrastructure." Moreover, there is no teaching in *Van Hoff* for a program to automatically broadcast an update message to other programs, *after* an update has been automatically downloaded by the first program from a remote site. Thus, there is no suggestion or motivation in *Van Hoff* for "broadcasting over a network an update message" within the context of in Claim 12. Absent such suggestion or motivation, the rejection is improper. *See* M.P.E.P., § 2143.01. Moreover, to the extent that the Examiner intends to take official notice that the elements of Claim 12 would be "apparent" or relies on "common wisdom practice" for a suggestion to modify the cited art, Applicant respectfully traverses this assertion and requests that the Examiner cite a reference in support of the Examiner's position pursuant to M.P.E.P. § 2144.03.

Claim 13, like Claim 9, recites restoring a first version of a program for operation at a network site when, after installation of a downloaded update, it is determined that the update is operating correctly. Thus, Claim 13 is patentable.

With respect to Claim 14, there is no suggestion or motivation in *Van Hoff* to combine the cited reference with an intrusion detection system. Absent such suggestion or motivation, the rejection is improper. *See* M.P.E.P., § 2143.01. To the extent that the Examiner intends to take official notice that it would be "common wisdom practice in

the art" to combine *Van Hoff* with an intrusion detection program or system, Applicant respectfully traverses this assertion and requests that the Examiner cite a reference in support of the Examiner's position pursuant to M.P.E.P. § 2144.03.

Similar to Claims 1 and 14, Claims 16 and 22 teach distribution of a intrusion detection system and are patentable over the cited art, as are their dependent Claims 17-21 and 23-24, respectively. In addition and similar to Claim 3, Claim 18 teaches aging a first set of intrusion detection signatures. Thus, Claims 16-24 are patentable.

New Claims

Claims 25-26 have been added to now fully claim the present invention. Applicant submits that no new matter is added by this amendment.

Conclusions

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicant respectfully requests full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicant stands ready to conduct such a conference at the convenience of the Examiner.

A check in the amount of $516.00 is enclosed to cover the fee for additional claims. Applicant believes that no additional fees are due, however, if it is determined that additional fees are due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Terry J. Stalford
Reg. No. 39,522

2001 Ross Avenue
Dallas, Texas 75201-2980
(214) 953-6477

Date: 4/27/01

CORRESPONDENCE ADDRESS:
Baker Botts L.L.P.
2001 Ross Avenue, Suite 600
Dallas, TX 75201-2980

Marked-Up Version of Claim Amendments

For the convenience of the Examiner, all claims have been presented whether or not an amendment has been made. The claims have been amended as follows:

IN THE CLAIMS

Please amend the claims as follows.

1. **(Amended)** A method for updating a first version of **[a] an intrusion detection** program operating at a network site, comprising:

in response to an automated event, automatically downloading from a remote site any update for the **intrusion detection** program;

installing a downloaded update to generate a second version of the **intrusion detection** program; and

operating the second version of the **intrusion detection** program in place of the first version at the network site.

2. The method of Claim 1, wherein the automated event is a timed event.

3. **(Amended) [The method of Claim 2, further comprising] A method for updating a first version of a program operating at a network site, comprising:**

aging the first version of the program;

[and wherein the timed event is] automatically downloading from a remote site any update for the program in response to the first version reaching a specified age**;**

installing a downloaded update to generate a second version of the program; and

operating the second version of the program in place of the first version at the network site.

4. The method of Claim 3, wherein the specified age is less than or equal to twenty-four hours.

5. The method of Claim 2, wherein the timed event occurs at least once a day.

6. **(Amended)** The method of Claim 1, the act of automatically downloading from the remote site any update for the **intrusion detection** program comprising:

automatically connecting to the remote site in response to the automated event;

automatically determining whether the remote site includes an update for the **intrusion detection** program; and

in response to the remote site including an update, automatically downloading the update from the remote site.

7. The method of Claim 1, further comprising downloading the update in an encrypted format and decrypting the downloaded update prior to installation.

8. The method of Claim 1, further comprising authenticating the downloaded update prior to installation.

9. **(Amended)** **[The method of Claim 1, further comprising] A method for updating a first version of a program operating at a network site, comprising:**

in response to an automated event, automatically downloading from a remote site any update for the program;

installing a downloaded update to generate a second version of the program;

after installation of the downloaded update, determining whether the second version of the program is operating correctly;

in response to correct operation of the second version, operating the second version of the program in place of the first version at the network site; and

in response to incorrect operation of the second version, restoring the first version of the program for operation at the network site.

10. **(Amended) [The method of Claim 1, further comprising] A method for updating a first version of a program operating at a network site, comprising:**

in response to an automated event, automatically downloading from a remote site any update for the program;

installing a downloaded update to generate a second version of the program; and

operating the second version of the program in place of the first version at the network site;

distributing the downloaded update to a disparate network site operating the first version of the program;

installing the downloaded update to generate the second version of the program at the disparate network site; and

operating the second version of the program in place of the first version at the disparate network site.

11. **(Amended)** **[The method of Claim 1, further comprising]** **A method for updating a first version of a program operating at a network site, comprising:**

in response to an automated event, automatically downloading from a remote site any update for the program;

installing a downloaded update to generate a second version of the program;

after installation of the downloaded update, determining whether the second version of the program is operating correctly at the network site;

in response to incorrect operation of the second version, restoring the first version of the program for operation at the network site; and

in response to correct operation of the second version at the network site:

distributing the downloaded update to a disparate network site operating the first version of the program;

installing the downloaded update to generate the second version of the program at the disparate network site; and

operating the second version of the program in place of the first version at the disparate network site.

12. **(Amended)** **[The method of Claim 1, further comprising]** **A method for updating a first version of a program operating at a network site, comprising:**

in response to an automated event, automatically downloading from a remote site any update for the program;

installing a downloaded update to generate a second version of the program; and

operating the second version of the program in place of the first version at the network site;

broadcasting over a network an update message;

receiving in response to the update message a request for the downloaded update from each of a plurality of disparate network sites operating the first version of the program;

distributing the downloaded update to the disparate network sites requesting the downloaded update;

installing the downloaded update to generate the second version of the program at each of the disparate network sites; and

operating the second version of the program in place of the first version at each of the disparate network sites.

13. The method of Claim 12, further comprising:

receiving a recovery event at one of the network sites;

automatically restoring the first version of the program at the network site at which the recovery event was received;

broadcasting a recovery message from the network site over the network; and

automatically restoring the first version of the program at each of the remaining network sites operating the second version of the program.

14. The method of Claim 1, wherein the program is a set of intrusion detection signatures for an intrusion detection sensor.

15. **[The method of Claim 1, wherein the remote site is]**

A method for updating a first version of a program operating at a network site, comprising:

in response to an automated event, automatically downloading from an Internet web page **any update for the program;**

installing a downloaded update to generate a second version of the program; and

operating the second version of the program in place of the first version at the network site.

16. A method for automatically updating an intrusion detection system having a plurality of distributed intrusion detection sensors each operating with a first set of intrusion detection signatures, comprising:

in response to a specified event, automatically downloading from a remote site any update for the intrusion detection signatures;

distributing a downloaded update to each sensor;

installing the downloaded update to generate a second set of intrusion detection signatures for each sensor; and

operating each sensor with the second set of intrusion detection signatures.

17. The method of Claim 16, wherein the specified event is a timed event.

18. The method of Claim 17, further comprising:

aging the first set of intrusion detection signatures; and

wherein the timed event is the first set of intrusion detection signatures reaching a specified age.

19. The method of Claim 18, wherein the specified age is less than or equal to twenty-four hours.

20. The method of Claim 17, wherein the timed event occurs at least once a day.

21. The method of Claim 16, the act of automatically downloading from the remote site any update for the program comprising:

automatically connecting to the remote site in response to the timed event;

automatically determining whether the remote site includes an update for the intrusion detection signatures; and

in response to the remote site including an update, automatically downloading the update from the remote site.

22. An intrusion detection system, comprising:

a private network including a plurality of sites connected to a public network, each site including an intrusion detection sensor operating with a first set of intrusion detection signatures; and

each of the intrusion detection sensors operable to automatically download from a remote site any update for the intrusion detection signatures in response to a specified event, to install a downloaded update to generate a second set of intrusion detection signatures, to operate with the second set of intrusion detection signatures, and to distribute the downloaded update to the remaining intrusion detection sensors for installation.

23. The system of Claim 22, wherein the specified event is an automated event.

24. The system of Claim 23, wherein the automated event is a timed event.